

基于可信推荐节点集合的 P2P 信誉模型

孙秋景¹, 曾凡平^{1,2}, 曹 勇^{1,2}

(1. 中国科学技术大学计算机科学与技术学院, 合肥 230026; 2. 安徽省计算与通讯软件重点实验室, 合肥 230026)

摘 要: 针对现有模型在节点行为变化时对诚实推荐节点的误判问题, 提出一种基于可信推荐节点集合的 P2P 信誉模型。在该模型中, 节点依据其推荐性能被划分为 2 个集合: 可信推荐节点集合及考察节点集合。计算节点信誉值时仅使用前者的推荐信息, 对后者中的节点进行实时考察以纠正被误判的诚实节点。网络节点依据其推荐性能的变化在 2 个集合内动态转化。仿真实验结果验证了该模型的有效性。

关键词: 对等网络; 信誉模型; 可信; 推荐

P2P Reputation Model Based on Credible Recommendation Node Set

SUN Qiu-jing¹, ZENG Fan-ping^{1,2}, CAO Yong^{1,2}

(1. School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China;

2. Anhui Province Key Lab of Software in Computing and Communication, Hefei 230026, China)

【Abstract】 A credible recommendation node set-based reputation model is proposed in this paper which solves the problem in the existent models that the miscarriage of justice for the honest recommenders when peers change their behavior. It divides the recommenders into two sets: the credible recommender set and the set to be taken a further look. The recommendations from the former set constitute the computation of peers' reputation value. The behavior of the latter set is observed to correct the honest recommender that has been done wrong. Peers transform dynamically between these two sets according to their recommendation performance. Experimental results show the model's validity.

【Key words】 P2P network; reputation model; credible; recommendation

1 概述

在 P2P 网络中, 节点间缺少必要的信任关系, 安全问题十分突出。基于信誉机制的信任模型能够对节点间建立信任关系, 一定程度上解决了 P2P 网络的安全问题。推荐节点在信誉系统中起着至关重要的作用^[1]。

推荐节点诚实性的检测方法大体可分为如下 3 种^[1]: (1)认为节点信誉值越高推荐越可信, 反之亦然, 该方法难于抵御信誉值较高节点对竞争者的诋毁攻击; (2)文献[2]认为大多数节点的推荐为真实的, 然而当节点行为改变(从可信变到不可信或者相反)时, 反馈该节点新的信任行为的诚实节点由于与主流观点不一致会被误判^[1]; (3)依据节点推荐信息与实际交易结果是否一致判断其推荐的诚实性^[3], 当交易节点的行为变化时, 反馈该节点变化前信任行为的诚实节点同样会被误判。已有模型没有考虑节点行为变化对系统诚实性检测的影响^[1], 一旦待交易节点行为改变就会对诚实节点造成不同程度的误判, 降低了其对系统进行推荐的能力, 进而影响信誉系统中信誉值计算的准确性。

为解决上述的误判问题, 本文提出一种有效的基于可信推荐节点集合的信誉模型(Credible Recommender Set-Based Trust Model, CRBTrust)。

2 信誉评估模型

本节首先简要给出直接信任值的计算方法, 然后重点阐述全局信誉值的计算及推荐节点考察机制, 最后详细阐述推荐节点的更新策略。

设时刻 t , 网络中某节点 i 欲与节点 j 进行交易。节点 i 仅依据自身与 j 的交易经验计算得到 j 的信任值, 称之为直接

信任值, 记为 D_{ij}^t 。而节点 i 综合自己及其他节点对 j 的推荐反馈, 经过计算得到 j 的综合信任值, 称为 j 的全局信誉值, 记为 Re_{ij}^t 。

在一次交易中依据节点角色的不同将其分为如下 3 类:

- (1)源节点: 发起交易请求的节点。
- (2)目标节点: 源节点将要与之发生交易的节点。
- (3)推荐节点: 向源节点反馈目标节点信任情况的节点。

2.1 直接信任值的计算

设时刻 t 、节点 i 对节点 j 提供服务的评分为 s_{ij}^t (s_{ij}^t 为 0 或 1, 分别代表满意及不满意的服务)。考虑到信任随时间的衰减性^[2], 本文引入时间衰减因子(记为 λ , $0 < \lambda < 1$, 为实数)的概念。 t' 为时间窗口 $win = [t_{start}, t_{end}]$ 内 i 与 j 某次交易发生的时间, t 为当前时间, 则 i 对 j 的直接信任值为:

$$D_{ij}^t = \sum_{t'=t}^{t'} \lambda^{t-t'} s_{ij}^{t'} \quad (1)$$

2.2 全局信誉值的计算

当源节点 i 与目标节点 j 在时间窗口 win 内无交易记录或交易不充分时会收集其他节点对 j 的推荐信息。本文采用基于权重的方法^[4]整合网络中节点的推荐信息。设推荐节点集合为 RC , 则 j 在时刻 t 的全局信誉值如式(2)所示:

$$Re_{ij}^t = \sum_{k \in RC} Cr_{ik \rightarrow j}^t D_{kj}^t / \sum_{k \in RC} Cr_{ik \rightarrow j}^t \quad (2)$$

作者简介: 孙秋景(1984 -), 女, 硕士研究生, 主研方向: 信息安全; 曾凡平, 副教授; 曹 勇, 硕士研究生

收稿日期: 2010-02-20 **E-mail:** billzeng@ustc.edu.cn

其中, $Cr_{ik \rightarrow j}^t$ 表示节点 i 对节点 k 推荐信息的信任程度, 称为推荐可靠性。

节点出于自身利益会进行虚假推荐。为了有效过滤恶意推荐节点及减少对诚实节点的误判, CRBTrust 模型在每个节点本地存储一个“推荐节点考察表”(简称考察表), 用于存储进行过错误推荐的节点。

由于错误推荐被列入考察表中的节点有如下 2 类: 恶意推荐节点; 诚实节点, 但目标节点行为变化造成其推荐信息与实际交易结果不一致的节点。对于前一类节点应当一直将其保留在考察表中, 而对于后一类节点应当使用相应机制将其从考察表中移除, 以备日后继续使用其推荐信息。出于安全性考虑, 本文仅使用未落入考察表中节点(称之为可信推荐节点)的推荐信息计算目标节点信誉值。设时间窗口 win 内与目标节点交易过的节点集合为 R , 则式(2)中推荐节点集合 RC 为集合 R 去除考察表 RT 中节点的部分, 即 $RC = R \setminus RT$ 。

为了更准确地度量节点推荐的准确性, 设 $win_s = [t_{start}, t_{end}] (t_{start} > t_{start})$ 为比正常时间窗口 win 小的子窗口。若 win_s 内节点 k 与节点 j 交易过, 则认为 k 对 j 近期行为的反馈越准确, 推荐可靠性也越高, 如式(3)所示。

$$Cr_{ik \rightarrow j}^t = \begin{cases} 1 & \text{when peer } k \text{ trade with peer } j \text{ during } win_s \\ 0.5 & \text{otherwise} \end{cases} \quad (3)$$

此外, 为了防止恶意节点频繁作恶, 本模型引入交易节点黑名单机制^[5]。若 win 内节点提供不满意服务次数超过 F_{MAX} , 则将其加入本地“交易黑名单”中, 以后不再与之交易。

2.3 推荐节点考察表

设节点进行交易时要求目标节点信誉值大于 T_α 。对于某推荐节点 k , 设其反馈目标节点 j 的信任值为 D_{kj} , 实际交易中节点 j 提供的服务为 s_j (0 或 1)。若 $(D_{kj} - T_\alpha) \cdot (s_j - T_\alpha) > 0$, 即 k 对 j 可信度的推荐值与实际交易中 j 的可信度一致, 则认为 k 进行了正确的推荐。反之, 认为 k 的推荐错误。

当节点推荐错误时将其放入本地“推荐节点考察表”中。该表的存储结构如表 1 所示。

表 1 推荐节点考察表

推荐节点 ID	重用位	考察时间 T	失败记录<目标节点 ID, 标记位>			
Id_2	1	N_2	< $Id_1, 0$ >	< $Id_3, 1$ >	< $Id_8, 1$ >	...
Id_5	1	N_5	< $Id_3, 1$ >	< $Id_4, 0$ >	< $Id_{10}, 1$ >	...
Id_7	0
...

其中, 重用位(0,1)标记是否对该节点继续进行考察: 重用位为 1 的节点, 实时向其发起推荐请求, 考察其推荐的正确性, 并更新考察表项, 以确定该节点是否为被误判的诚实节点。对于重用位为 0 的节点, 认为其完全不可信, 不再向其发起推荐请求。

考察时间: 节点在考察表中待考察次数。交易结束后, 依据其推荐是否正确减少或增加其考察时间。考察时间为 0 时, 将节点从考察表中删除。失败记录<目标节点 ID, 标记位>: 其中, 目标节点 ID 代表了某次推荐的目标节点 ID。标记位(0, 1)记录了错误推荐的原因: 0 表示该节点反馈的目标节点信任值大于 T_α , 而实际交易中目标节点提供不满意服务; 1 表示反馈的目标节点信任值小于等于 T_α , 实际交易中目标节点提供满意服务。

2.4 推荐节点更新机制

交易(设源节点为 i , 目标节点为 j)结束后, 源节点依据交易结果对推荐节点进行更新处理。

对可信推荐节点: 若其推荐错误, 将其加入考察表中(自身除外), 重用位置 1, 考察时间置为 U_T 。依错误推荐原因在失败记录中添加记录 < $Id_j, 1$ > 或 < $Id_j, 0$ >。若其推荐正确, 则不进行处理。

对于考察表中的节点: 若其推荐正确, 则将其考察时间减 1。若其推荐错误, 首先查看失败记录中是否存在记录 < $Id_j, 1$ > 或 < $Id_j, 0$ >。若存在则不累加其考察时间, 反之将其考察时间增加 U_T , 并在失败记录表项中依错误推荐原因添加记录 < $Id_j, 1$ > 或 < $Id_j, 0$ >。本模型不因节点对同一目标节点的多次错误推荐而重复累加其考察时间。原因如下: 对于因目标节点行为变化而反馈了过时推荐信息的诚实节点, 如果此时仍未与该节点发生新的交易, 必定再次反馈过时信息, 造成推荐错误。另外, 本模型为考察时间设定一个上限 T_{MAX} , 以防止网络中恶意节点频繁改变行为, 造成诚实节点不断累加考察时间最终陷入考察表中难以移出。

若本次交易中目标节点 j 提供了不满意服务, 则 j 很可能为恶意节点。搜索考察表中所有重用位为 1 的节点的失败记录中是否存在 < $Id_j, 1$ > 的记录。若存在, 则认为该推荐节点之前在很大程度上被误判了, 将其立即从考察表中移除。然而本文不依据记录 < $Id_j, 0$ > 对推荐节点进行后期修正。这是因为当标记位为 0 时, 推荐节点存在两种可能: 一种是该节点为恶意节点, 并夸大目标节点的信任值; 另一种是该节点为诚实节点。但由于目标节点的行为变化而被误判。所以, 很难依据目标节点以后的交易行为判别推荐节点的类别。

对处于交易黑名单中的节点, 其推荐同样不可信, 将其加入考察表中, 设置重用位为 0。以后既不与它进行交易, 也不向其发送推荐请求。

3 仿真实验分析

为了验证模型性能, 本文设计了 2 组实验并与 CF^[3]模型进行比较。设网络中有 100 个节点, 好节点、普通恶意节点及合谋恶意节点所占比例为 0.6, 0.2, 0.2。其中, 好节点提供满意服务并诚实推荐; 普通恶意节点进行虚假反馈: 当某节点的信任值大于 T_α 时反馈 0, 反之反馈 1; 合谋恶意节点反馈同类节点的信任值为 1, 反馈其他节点的信任值为 0。两种类型的恶意节点以周期性 N 提供不满意服务(第 1 轮交易提供满意服务)。随机选择交易节点, 若该节点满足要求则与之交易, 否则重新选择交易节点。CRBTrust 模型要求: 交易节点不在源节点的交易黑名单中且信誉值大于 T_α 。对于 CF 模型, 交易节点的综合信任评价需大于 0 且综合不信任评价等于 0。实验中两模型参数设置如表 2。

表 2 仿真参数表

参数及描述	默认值
交易节点信誉值阈值 T_α	0.5
时间窗口 win	100
子时间窗口 win_s	10
时间衰减因子 λ	0.5
单位考察时间 U_T	2
考察时间最大值 T_{MAX}	6
不满意服务次数阈值 F_{MAX}	2
CF 模型中信任向量长度 L	32
CF 模型中最可信推荐节点数 θ	4

3.1 诚实推荐节点误判率

本组实验测试节点行为变化时($N=5$)诚实推荐节点的误判率。设每次交易均由好节点发起请求。交易结束后,对于推荐错误的节点:CF模型对其进行标记,以后全网均不使用该节点的推荐信息;对于CRBTrust模型,源节点将其加入本地考察表中。诚实节点的误判率如图1所示。其中,被误判的诚实节点在CF模型中为被标记的诚实节点,CRBTrust模型中为考察表中的诚实节点。

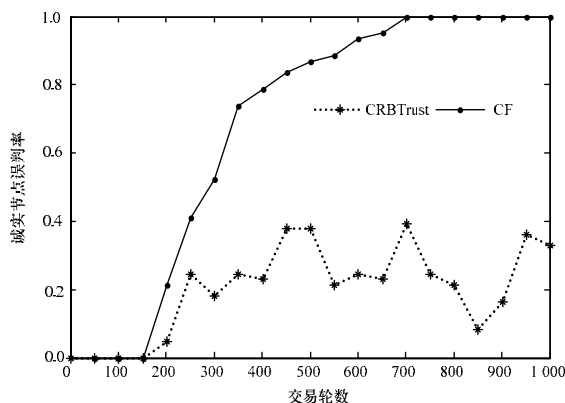


图1 诚实推荐节点误判率

由图1可见,本文模型中诚实节点的误判率远远小于CF模型。这是由于CF模型没有考虑节点行为的变化对推荐节点诚实性检测的影响^[1],随着交易的进行被误判的诚实节点逐渐增多。而本模型对错误推荐节点进行后期考察,正如2.4节所述,能够在一定程度上纠正被误判的诚实节点,削弱了节点行为的变化对诚实节点的影响。

3.2 成功交易率

本组实验以 $N=2$ 为例比较两模型成功交易率。网络中节点随机进行交易,并随机选择一好节点统计其成功交易率情况。如图2所示,本文模型有更好的性能。由于恶意节点行为摇摆,使得CF模型中诚实节点被误判,其推荐可靠性(可靠因子-不可靠因子)逐渐减低,最终导致计算得到的目标节点信誉值与其实际可信度相差较大,这加大了选取恶意节点作为交易节点的概率,最终使得系统成功交易率受到影响。而CRBTrust模型能够对被误判的诚实节点进行纠正,最终提升了系统的成功交易率水平。

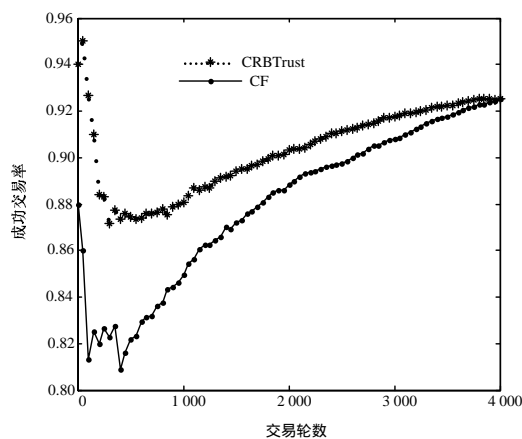


图2 成功交易率

4 结束语

本文提出的信誉模型将推荐节点划分为2个集合:可信推荐节点集合及考察节点集合,并对后者进行实时考察。本模型有效降低了节点行为变化对推荐节点诚实性检测的影响,提升了系统成功交易率。进一步完善推荐节点的考察机制及分析网络中节点间的关系是以后要做的工作。

参考文献

- [1] Farag A, Ahmad R. The Effect of Behavior Change on Honesty Checking in Peer-to-Peer Systems[C]//Proc. of the 6th Annual Conference on Privacy, Security and Trust. Fredericton, New Brunswick, Canada: [s. n.], 2008.
- [2] Dong Jianquan, Tan Chao, Zhang Yunqi. A Reputation Evaluation Method in P2P Anonymous Environment[C]//Proc. of the 9th International Conference for Young Computer Scientist. Zhangjiajie, China: [s. n.], 2008: 1516-1521.
- [3] Selcuk A, Uzun E, Pariente M. A Reputation-based Trust Management System for P2P Networks[J]. International Journal of Network Security, 2008, 6(3): 235-245.
- [4] 席菁, 王源, 陆建德. 基于信任和推荐的P2P信誉模型[J]. 计算机工程, 2009, 35(4): 143-145.
- [5] Li Mingchu, Ren Yizhi, Kouichi S, et al. Granularity Considering in a Trust Model for P2P Networks[C]//Proc. of the 22nd International Conference on Advanced Information Networking and Applications. Ginowan, Okinawa, Japan: [s. n.], 2008: 307-312.

编辑 陈文

(上接第141页)

- [5] 章志明, 邓建刚, 余敏. 一种安全有效的多轮电子拍卖协议[J]. 计算机工程, 2006, 32(10): 157-158.
- [6] Franklin M K, Reiter M K. The Design and Implementation of a Secure Auction Service[J]. IEEE Trans. on Software Engineering, 1996, 22(5): 302-312.
- [7] Sakurai K. A Bulletin-board Based Digital Auction Scheme with Bidding Down Strategy[C]//Proc. of CryptTEC'99. Hong Kong, China: [s. n.], 1999.
- [8] Kikuchi H. M+1 St-price Auction Protocol[C]//Proc. of the 5th International Conf. on Financial Cryptography. Grand Cayman, British West Indies, UK: [s. n.], 2002.

- [9] Brandt F. Fully Private Auction in a Constant Number of Rounds[C]//Proc. of the 7th Annual Conf. on Financial Cryptography. Guadeloupe, Mexico: [s. n.], 2003.
- [10] Sakurai K, Miyazaki S. An Anonymous Electronic Bidding Protocol Based on a New Convertible Group Signature Scheme[C]//Proc. of ACISP'00. Brisbane, Australia: [s. n.], 2000.
- [11] Yi Mu, Varadharajan V. An Internet Anonymous Auction Scheme[C]//Proc. of ICISC'00. Seoul, Korea: [s. n.], 2000.

编辑 顾姣健